ABSTRACT OF THE DISCLOSURE

METHODS AND APPARATUS FOR NETWORK MESSAGE TRAFFIC REDIRECTION

Conventional methods of addressing a Distributed Denial of Service attack include taking the target node offline, and routing all traffic to an alternate countermeasure, or "sinkhole" router, therefore requiring substantial lag time to reconfigure the target router into the network. In a network, a system operator monitors a network for undesirable message traffic. Upon a notification of such undesirable message traffic, traffic is rerouted to a filter complex to separate undesirable traffic. The filter complex establishes an alternate route using a second communications protocol, and uses the alternate route to redirect the desirable message traffic to the target node. The use of the second protocol avoids conflict between the redirected desirable traffic and the original, or first, protocol which now performs the reroute. In this manner, the filter complex employs a second alternate communications protocol to reroute and redirect desirable message traffic to the target node while diverting undesirable message traffic, and therefore avoids widespread routing configuration changes by limiting the propagation breadth of the second protocol.